cpl.thalesgroup.com

THALES
Building a future we can all trust

Major North American retail chain leverages Luna HSMs to implement comprehensive data security and key management best practices

A major North American grocery chain with thousands of stores nationwide wanted to improve its cyber security defenses and lower its risk of data breach. Specifically, the retail chain wanted to implement data-centric security and key management best practices to protect credit card and personally identifiable information (PII) data on multiple platforms, some of which are shared by the group's pharmacy and retail banking operations. The retailer also wanted to improve its Payment Card Industry (PCI) compliance posture.

Challenge

The retailer had multiple security platforms managing encryption for databases, identity and access management, and Public Key Infrastructure (PKI) use cases. The company wanted to centralize key management for all these different systems on a highly secure Hardware Security Module (HSM) platform.

Solution

The retailer implemented Thales Luna HSMs to protect encryption keys from multiple systems, including Oracle databases leveraging Transparent Data Encryption (TDE) and CyberArk Privileged Access Management. Luna HSMs centralized all key management for all use cases in a single highly secure root-of-trust.

Thales Luna HSMs

Thales Luna HSMs are dedicated crypto processors specifically designed to protect the crypto key lifecycle. HSMs act as trust anchors that protect the cryptographic infrastructure of some of the most security-conscious organizations in the world by securely managing, processing, and storing cryptographic keys inside a hardened, tamper-resistant device. Enterprises use HSMs to protect transactions, identities, and applications, because HSMs excel at securing cryptographic keys and provisioning encryption, decryption, authentication, and digital signing services for a wide range of applications.

FIPS 140-2 Level 3 Luna HSMs provide the highest level of security by always storing cryptographic keys in hardware. They provide a secure crypto foundation because the keys never leave the intrusion-resistant, tamper-evident, common-criteria validated appliance. Since all cryptographic operations occur within the HSM, strong access controls prevent unauthorized users from accessing sensitive cryptographic material. Thales also implements operations that make the deployment of secure HSMs as easy as possible. They are integrated with Thales Crypto Command Center for quick and easy crypto resource partitioning, reporting, and monitoring.

> "The retail chain established comprehensive data security and key management best practices, improved PCI compliance, and expanded the Luna HSM-based security framework into new use cases."

Results

The retail chain established comprehensive data security and key management best practices, improved PCI compliance, and expanded the Luna HSM-based security framework into new use cases.

Established security best practices

Deployed key management best practices based on Luna HSMs for the entire group including grocery, pharmacy, and the retail bank.

Enhanced PCI compliance

Improved compliance by protecting essential encryption key material used in multiple platforms.

Scaled into new use cases

Expanded their security framework into multiple new use cases, ensuring a long-term customer relationship with Thales for over a decade.

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

Contact us – For all office locations and contact information, please visit cpl.thalesgroup.com/contact-us